Transparency Today

Bakir, Vian

Published: 06/01/2015

Publisher's PDF, also known as Version of record

Transparency Today: Exploring the Adequacy of Sur/Sous/Veillance Theory and Practice 6 January 2015

Seminar Summary

This summary is based on detailed seminar summaries provided by PhD students Abigail Blyth, Aberystwyth University; George Petry, University of South Wales; and Tiewtiwa Tanalekhapat, Aberystwyth University

Introduction by Dr Vian Bakir and Dr Andrew McStay: The seminar began with an in-depth discussion of three types of transparency; two originally identified by Bentham: Liberal and Radical Transparency, and one coined by McStay, that appears increasingly pertinent to today's society: Forced Transparency, or transparency without consent or choice.

Keynote 1: Professor Steve Mann, University of Toronto, introduced some key concepts, including sousveillance, surveillance, equiveillance, and priveillance. Mann argues that surveillance is hypocritical, centralised, secretive and corrupt whereas sousveillance has integrity, openness and is distributed. He predicted a time in the future when an 'equiveillance point' will be reached with an equal number of cameras carrying out surveillance, and the same amount of cameras being used by the public as wearable media carrying out sousveillant activity. This will, he argues, in due course lead back to a situation where everyone is wearing cameras, thereby negating the need for, and legitimacy of, surveillance. Slides are available on: http://wearcam.org/html5/mannkeynotes/priveillance.htm

In the lively **Roundtable on Sousveillance** that followed, the group discussed whether the continued focus on the visual aspects (i.e. the 'veillance' part) of surveillance was legitimate. Recent events such as the Edward Snowden revelations has shown that surveillance encompasses much more, including an examination of mass data – dataveillance – and sousveillance might not be able to fully counter that surveillance. The discussion then turned to the possibility of having sousveillant data transmigrate into surveillant data, if it falls into the wrong hands; the commodification of data, and the issues of 'dark corners of power' that fall beyond the reaches of sousveillance. The legal and technological aspects, including the law's fairly limited interpretation of the right to privacy, and issues of encryption and 'making sense' of big data, were discussed at length.

Keynote 2: Professor Kirstie Ball, Open University, highlighted the blurring of the lines between the state and the private sector in national security matters. To protect national security, the UK Border Agency created an obligation on airlines to provide a securitised

data flow of passport information of those booked on planes, and taking flights. By reflecting on the concept of transparency from the research project, Ball addresses the notion of transparency veillance, in which transparency consequently has become multilayered and politicised. She argues that to securitise something is to render it dangerous, and commercial activities are generally shot through with insecurities.

The **Roundtable on Surveillance** began with a scintillating short presentation on the work of PlanetLabs - https://www.planet.com/ - a satellite imaging company. This further highlighted the role of the private sector in the collection and dissemination of data and how they interact with respective national legislation in this field. PlanetLabs is based in the USA and the US Government has the ability to access their satellite images and equally to stop them to photographing certain areas of the world. From an intelligence studies perspective, this continues to raise questions in relation to the interaction between governments and private companies when matters of national security are involved. It also highlights the problematical debate witnessed within the UK Intelligence and Security Committee's Annual Reports on accountability over matters concerning national security. Some discussion ensued on whether the dichotomy between surveillance and sousveillance remains useful given the uncertainty of data flows regardless of their origin.

Policy Recommendations

1. There is a need for politics students, academics, and professionals to be technologically aware as well as for computer science and engineering students, academics, and professionals to be politically aware as disciplines continue to intersect.
2. Those involved in data creation and storage need to be mindful of the possibility of that data being misused, intercepted, or commodified by others – with or without their consent. Users need to consider how data can be controlled and accessed, and what use can be made of data once created.
3. Governments must be aware of the implications of outsourcing surveillance to private entities, both in terms of the negative impacts on competition that can result (as highlighted by Ball *et al.*) and more broadly of the fact that by securitising an activity, it is implicitly rendered dangerous. There are important implications for the private sector and customer relations, if private companies are co-opted into a policing function.
4. A deeper engagement with the concept of privacy and what it means in today's society needs to be undertaken, from political, journalistic, legal and philosophical perspectives, amongst others. Are technological tools to prevent surveillance sufficient to protect privacy or are we entering an arms' race of technological techniques of surveillance and counterveillance (ie measures to block any type of watching)?
5. The extent to which individuals can avoid interference with their privacy in an increasingly technological society, and the extent to which sousveillance can counteract surveillance, is worthy of further in-depth examination. In particular, is there value in sousveillance without meaningful evidence of accountability?